"PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS"

La presente invención hace referencia al procedimiento arriba indicado, con el cual resulta imposible la duplicación operativa de los mismos de manera fraudulenta. Tal como se detallará en lo sucesivo, el procedimiento que se describirá a continuación ofrece numerosas ventajas.

Aunque en la presente memoria se hace referencia esencialmente al caso en el que los documentos que se desean obtener son tickets, se entiende que el procedimiento objeto de la presente invención también es aplicable a otros tipos de documentos más generales, tal como se explicará más adelante.

Hoy en día es posible el encargo o la reserva de tickets tales como billetes de avión, billetes de tren, localidades de espectáculos y similares mediante sistemas de tele-venta. El procedimiento para el pago de los mismos es variado, pudiéndose realizar mediante el cargo a una tarjeta de crédito, a una cuenta a través de una entidad bancaria o similar.

Sin embargo, para recoger el ticket comprado de este modo era necesario que éste fuera enviado al destinatario por correo o mediante un servicio de mensajería, lo cual suponía un aumento en los costes de emisión y una incomodidad para el usuario si debía desplazarse para recoger los tickets.

Hasta ahora, la recogida del ticket se venía realizando de esta manera debido principalmente al hecho de que la autenticidad de este tipo de documento está basada en alguna característica del soporte (el papel) o del método de impresión para dificultar la falsificación del mismo. Esto impide que sea el propio usuario el que pueda obtener una copia impresa del documento.

Como alternativa a este procedimiento la técnica

anterior propone diversos sistemas de expedición de tickets de manera remota, los cuales se describen resumidamente a continuación.

Un primer sistema es el que se describe, en mayor o menor medida, en los documentos nº WO01/61577 A2, WO00/74300 A1, WO00/45348, WO200161577,WO2000744300, WO200045348, US5598477, el cual está basado esencialmente en la codificación de los datos que se consideran relevantes y su posterior cifrado, bien mediante técnicas de clave simétrica o asimétrica. El resultado de dicho cifrado se imprime en forma de código de barras o similar para poder realizar una comprobación automática cuando el ticket haya de ser validado. Este sistema imposibilita la generación de tickets por quien desconoce la clave de cifrado (si se usa criptografía de clave asimétrica, la clave secreta del algoritmo). Sin embargo, presenta el inconveniente de que es posible realizar copias de un ticket ya emitido y, por lo tanto, resulta necesario utilizar mecanismos adicionales de seguridad, tal como el control en línea de los tickets validados, la inclusión de información personal contrastable (DNI, pasaporte o similar) en el código cifrado (para aquellos tickets que presenten una fecha y un lugar fijos de utilización), etc. Este sistema es especialmente ineficaz en el caso de tickets que pueden ser utilizados en múltiples lugares y en un amplio abanico de fechas, como pueden ser bonos de noche en hoteles, bonos de transporte público, etc, así como en lugares de afluencia masiva, en los que el tiempo requerido para la comprobación de la identidad del portador resulta un serio inconveniente. Por todos estos motivos, este sistema no ha tenido demasiada implantación en la práctica.

Otro sistema es el que se describe, en mayor o menor medida, en los documentos nº EP0969426 A1, EP0829828 A, EP969426, JP11306397, EP309318 y otros, el cual está

basado en la grabación, en un dispositivo del tipo tarjeta inteligente, de la información del ticket. Debido a que el dispositivo de grabación (tarjeta) permite el uso de técnicas criptográficas para la identificación fuerte y presenta una gran robustez frente a la violación de la información que almacena, resulta prácticamente imposible duplicar el ticket, quedando la unicidad del mismo garantizada. Por lo tanto, resultan innecesarios tanto el control en línea de la validación del ticket como la identificación del portador cuando se consume. Sin embargo, este sistema presenta el inconveniente de que requiere que el usuario disponga de un periférico de grabación de tarjetas inteligentes en su casa, lo que encarece en gran medida el coste del sistema y hace que en la práctica no se utilice.

Una alternativa a los sistemas de expedición de tickets de manera remota es la que se propone con el nuevo procedimiento objeto de la presente invención, con el cual se consigue solventar los inconvenientes de los sistemas conocidos. La invención propone un nuevo procedimiento para la obtención de documentos (por ejemplo, tickets) típicamente en casa del usuario y su posterior validación automática. Con el procedimiento de la invención ya no es posible la duplicación operativa de los mismos (garantiza la unicidad) y hace innecesario que el usuario disponga de un lector/grabador de tarjetas inteligentes, lo que abarata y flexibiliza el sistema.

El procedimiento de la invención utiliza técnicas criptográficas robustas en conjunción con dispositivos verificadores portátiles, los cuales poseen capacidad de procesado y almacenamiento de información, presentan un alto grado de protección frente a lecturas y escrituras desautorizadas y dificultan en gran medida la duplicación fraudulenta.

Unos dispositivos verificadores portátiles que

resultan especialmente adecuados son las tarjetas inteligentes.

Aunque teóricamente resulta más adecuado el uso de criptografía de clave pública para la obtención de códigos de autenticidad (pues ello permite que en la fase de validación no se tengan que almacenar claves secretas), el tamaño de los códigos resultantes es sensiblemente superior al necesario si se emplea criptografía de clave secreta (simétrica). Si la forma final del documento no es impresa (soporte magnético, óptico, electrónico, etc.) este hecho no presenta mayor relevancia, pero si el documento ha de imprimirse, la lectura automática del código de autenticidad obligaría al uso de códigos de puntos, cuya lectura requiere aparatos más caros. Por este motivo, y para facilitar el soporte impreso, se prefiere el uso de criptografía de clave simétrica. Como contrapartida se tienen que utilizar dispositivos de almacenamiento seguro de claves en los verificadores, típicamente microprocesadores de seguridad.

La invención constituye un sistema seguro de expedición remota (típicamente por Internet desde un navegador) de documentos (típicamente tickets) y su validación mediante lectores automáticos (típicamente lectores de códigos de barras) capaces de leer/escribir en los dispositivos verificadores portátiles (típicamente tarjetas inteligentes). Por motivos de rapidez de lectura, robustez y versatilidad es recomendable que los dispositivos verificadores portátiles permitan la operación sin contactos.

Los elementos que intervienen en todo el procedimiento de la invención son los siguientes:

- emisor de dispositivos verificadores portátiles: es el encargado de proporcionar los dispositivos verificadores portátiles necesarios para la validación de los documentos.

- operador de dispositivos verificadores portátiles: realiza la parte del cifrado del documento que será descifrado por el dispositivo verificador portátil. Para poder realizar esta función las claves correspondientes deben de ser cargadas en el dispositivo verificador portátil. Un dispositivo verificador portátil puede soportar varios operadores de dispositivos verificadores portátiles. Un operador de dispositivo verificador portátil puede coincidir con un emisor.

- portal de documentos: es el encargado de proporcionar el interfaz necesario para la selección y, si procede, la compra del documento. Una vez seleccionado el documento el portal envía a un operador de lector la información adecuada para que sea cifrada con la clave del grupo de lectores/verificadores/grabadores que serán los encargados de validar el documento.

- operador de lector: es el encargado de realizar la parte del cifrado del documento que será descifrada por el citado grupo de lectores/verificadores/grabadores que serán los encargados de validar el documento. El operador de lector es el encargado de la gestión de las claves almacenadas en los lectores/verificadores/grabadores. Un operador de lector puede coincidir con un portal.

- lector/verificador/grabador: es el encargado de leer el código de autenticidad del documento, transmitirlo al dispositivo verificador portátil, recibir su respuesta, descifrarla con la clave correspondiente al operador de lector y validar o rechazar el documento.

- dispositivo verificador portátil: es el encargado de recibir el código de autenticidad del documento (transmitido por el lector/verificador/grabador), y si no ha sido previamente cancelado, descifrar con la clave correspondiente al operador de dispositivos verificadores portátiles,

incluirlo en su lista de cancelaciones y enviar al lector/verificador/grabador el resultado del descifrado.

El procedimiento de expedición y validación de documentos objeto de la presente invención se lleva a cabo mediante códigos de autenticidad y elementos verificadores portátiles con capacidad de procesado y almacenamiento de información y alta protección frente a lecturas o escrituras desautorizadas.

La particularidad de este procedimiento reside en el hecho de que el código de autenticidad se genera específicamente para un verificador portátil concreto, indicado de forma directa o indirecta por el solicitante del documento, de manera que es innecesario cualquier registro de información en el elemento verificador portátil hasta el momento de la validación del documento e imprescindible la participación activa de dicho elemento de verificación portátil para dicha validación, almacenando el verificador portátil una lista de los documentos que ha validado, de manera que es posible saber, al menos, si se trata de la primera validación.

El procedimiento de expedición y validación de documentos comprende las etapas de:

- generación del documento desde un portal de documentos codificándose los datos que se consideren relevantes para realizar una primera operación criptográfica con la clave correspondiente de un grupo de lectores/verificadores/grabadores que participan en la validación del documento y, concatenada a la primera, una segunda operación criptográfica que incluye la clave correspondiente del dispositivo verificador portátil asociado al documento, constituyendo el resultado de dichas operaciones criptográficas un código de autenticidad del documento incorporado al mismo; y

- comprobación del documento que comprende la lectura del código de autenticidad del mismo, realizándose

unas terceras operaciones criptográficas adecuadas para la verificación de las utilizadas en la generación del documento, siendo imprescindible la participación activa del dispositivo verificador portátil asociado para la validación del documento y almacenando el verificador portátil una lista de los documentos que ha verificado de manera que es posible saber, al menos, si se trata de la primera validación.

De acuerdo con una realización de la invención, la individualización de los dispositivos verificadores portátiles se realiza almacenando una o varias claves de dispositivo verificador portátil, siendo estas claves las de un algoritmo de cifrado simétrico o de clave secreta. Además, dicha primera y segunda operación criptográfica comprenden dos cifrados mediante un algoritmo criptográfico simétrico, uno con la clave del grupo de lectores/verificadores/grabadores que participan en la validación del documento y otro con la clave correspondiente del dispositivo verificador portátil asociado al documento; y las terceras operaciones criptográficas comprenden el descifrado, por parte del dispositivo verificador portátil con su clave correspondiente, del código de autenticidad del documento y el descifrado subsiguiente, por parte del citado lector/verificador/grabador con su clave correspondiente, realizándose ambos descifrados mediante algoritmos criptográficos simétricos.

Preferiblemente, la individualización de los dispositivos verificadores portátiles se lleva a cabo almacenando una o varias claves de dispositivo verificador portátil, siendo estas claves las secretas de un algoritmo criptográfico asimétrico o de clave pública. La citada primera y segunda operación criptográfica se basa en criptografía de clave pública que comprende una firma digital con una clave secreta, de la cual los citados

lectores/verificadores/grabadores que participan en la validación del documento conocen su correspondiente pública, y un cifrado con la clave pública correspondiente del dispositivo verificador portátil asociado al documento; y las terceras operaciones criptográficas se basan en criptografía de clave pública que comprenden un descifrado con la clave secreta correspondiente del dispositivo verificador portátil asociado al documento y una comprobación de firma, con la clave pública correspondiente almacenada en los lectores/verificadores/grabadores.

Alternativamente, la individualización de los dispositivos verificadores portátiles se lleva a cabo almacenando una o varias claves de dispositivo verificador portátil, siendo estas claves las secretas de un algoritmo criptográfico asimétrico o de clave pública. Dicha citada primera y segunda operación criptográfica se basa en criptografía de clave pública que comprende un cifrado con la clave pública de los lectores/verificadores/grabadores que participan en la validación del documento y un cifrado con la clave pública correspondiente del dispositivo verificador portátil asociado al documento. Las citadas terceras operaciones criptográficas se basan en criptografía de clave pública que comprenden un descifrado con la clave secreta correspondiente del dispositivo verificador portátil asociado al documento y una descifrado con la clave secreta de dichos lectores/verificadores/grabadores.

De acuerdo con otra característica alternativa de la presente invención, la individualización de los dispositivos verificadores portátiles se lleva a cabo almacenando una o varias claves de dispositivo verificador portátil, siendo estas claves las públicas de un algoritmo criptográfico asimétrico o de clave pública. La primera y segunda operación criptográfica se basan en criptografía

de clave pública que comprende una firma digital con la clave secreta correspondiente a la clave pública almacenada en los citados lectores/verificadores/grabadores que participan en la validación del documento y otra firma digital con la clave secreta correspondiente a la clave de individualización adecuada almacenada en el dispositivo verificador portátil asociado al documento, y las citadas terceras operaciones criptográficas se basan en criptografía de clave pública que comprende la comprobación de firma por parte del dispositivo verificador portátil asociado al documento con su clave de individualización adecuada y otra comprobación de firma con la clave pública correspondiente de los lectores/verificadores/grabadores.

Otra alternativa es que la individualización de los dispositivos verificadores portátiles se lleve a cabo almacenando una o varias claves de dispositivo verificador portátil, siendo estas claves las públicas de un algoritmo criptográfico asimétrico o de clave pública y que la primera y segunda operación criptográfica se basen en criptografía de clave pública que comprende un cifrado con la clave pública correspondiente a la clave secreta almacenada en dichos lectores/verificadores/grabadores que participan en la validación del documento y una firma digital con la clave secreta correspondiente a la clave de individualización adecuada almacenada en el dispositivo verificador portátil asociado al documento; y que dichas terceras operaciones criptográficas se basen en criptografía de clave pública que comprende una comprobación de firma por parte del dispositivo verificador portátil asociado al documento con su clave de individualización adecuada y un descifrado con la clave secreta correspondiente de los citados lectores/verificadores/grabadores.

Adicionalmente, el procedimiento de la invención

también comprende la comprobación, antes de validar el documento, de que éste no se encuentra en la lista de documentos validados.

También se realiza una indicación al lector/grabador/verificador de que el documento a validar se encuentra en la lista de documentos validados para que éste tome las medidas oportunas.

Se prevé asimismo la inclusión del documento en la lista de documentos validados en el caso de que el documento a validar no se encuentre en la misma, realizándose la operación criptográfica correspondiente a invertir y/o comprobar la operación criptográfica correspondiente al dispositivo verificador portátil, enviando el resultado al lector/grabador/verificador para que tome las medidas oportunas.

Ventajosamente, la autentificación criptográfica establecida entre el citado dispositivo verificador portátil y el lector/grabador/verificador es una autentificación criptográfica mutua fuerte.

Debe destacarse especialmente el hecho de que entre el dispositivo verificador portátil y el lector/grabador/verificador se establece una clave de sesión cooperativa y aleatoria utilizada para cifrar los mensajes pertinentes entre ambos.

Preferiblemente, la etapa de individualización de los dispositivos verificadores portátiles por parte de sus emisores se realiza mediante una o varias claves que se obtienen a partir del cifrado del número de serie con una o varias claves maestras elegidas por los operadores de dispositivos verificadores portátiles, de manera que la clave maestra de cada operador y el dispositivo verificador portátil corresponde con su identificador, apareciendo dicho identificador de una manera legible para el usuario.

De acuerdo con la invención, el citado

lector/verificador/grabador está adaptado para emitir una información admitiendo o rechazando el documento e informando de la causa.

Ventajosamente, las claves del lector/verificador/grabador son comunes a un conjunto de lectores.

Las claves almacenadas en los lectores/verificadores/grabadores se obtienen cifrando sus identificadores o parte de ellos con unas claves maestras elegidas por sus operadores.

Si los documentos presentan fecha de caducidad, ésta se incorpora en el código de autenticidad, de manera que pueden ser eliminados de la lista de documentos validados almacenada en dicho verificador portátil una vez que éstos han caducado.

Por otra parte, los citados dispositivos verificadores portátiles adquieren la fecha para borrar los documentos caducados de la lista de documentos validados por medio de un certificado digital emitido por una entidad competente.

La selección y obtención del documento y/o su código de autenticidad puede realizarse a través de Internet y el código de autenticidad del documento se puede enviar al teléfono móvil del usuario o una agenda electrónica o similar del usuario.

De acuerdo con otra característica de la invención, el código de autenticidad puede imprimirse mediante uno o varios códigos de barras. En el caso de varios códigos, éstos incluyen el orden correcto de lectura. Se prevé también que el código de autenticidad pueda imprimirse mediante un código alfanumérico o un código de puntos. El código de autenticidad puede imprimirse también en modo alfanumérico para poder realizar una entrada manual del mismo en caso de deterioro del código de lectura automática.

El procedimiento descrito garantiza la autenticidad y la unicidad de los documentos. Los cifrados del código de autenticidad se realizan utilizando un par de claves secretas. Esto asegura que no puedan generarse externamente documentos auténticos. La unicidad se consigue relacionando uno de los cifrados con el dispositivo verificador portátil. Si el documento se duplica por cualquier sistema, no se obtiene ningún resultado ya que el dispositivo verificador portátil, una vez que valida un documento, no vuelve a validarlo de nuevo. Por lo tanto, para sacar partido a la copia sería necesario duplicar el dispositivo verificador portátil y esto no es posible por sus características.

Por otra parte, es posible también la cancelación de documentos sin necesidad de transmisión de listas negras al lector/verificador/grabador. Para la cancelación, el titular del documento debe acudir a una oficina autorizada con el documento y el dispositivo verificador portátil. Para cancelar el documento, se cargará como anulado en el dispositivo verificador portátil de manera que, si el comprador ha guardado una copia del documento, no podrá usarlo puesto que ese dispositivo verificador portátil ya no lo validará.

La inclusión de listas de cancelación de documentos (si se desea que no se desborde la capacidad de almacenamiento del dispositivo verificador portátil) tiene varias implicaciones. Los documentos que caduquen deben incorporar la fecha de caducidad en el código de autenticidad, de manera que una vez hayan caducado puedan ser eliminados de la lista para liberar espacio. Los dispositivos verificadores portátiles deben incorporar un gestor de cancelaciones residuales, de manera que detecten los documentos caducados y realicen una limpieza a partir de la fecha obtenida de un certificado proporcionado por el lector/verificador/grabador. La fecha se obtiene de un

servidor central que certifica la misma mediante un sistema de clave pública. Dicho certificado, que puede ser emitido una única vez al día, se pasa al dispositivo verificador portátil que, después de comprobar su autenticidad, elimina de la lista los documentos cancelados que ya hayan caducado según la fecha certificada. Naturalmente un documento caducado no será nunca aceptado como válido.

Se trata de un sistema universal para múltiples servicios (espectáculos, transportes, abonos, cupones, cheques, boletos de lotería...), múltiples portales de Internet y múltiples operadores de dispositivos verificadores portátiles. Aunque el sistema es particularmente útil para el formato impreso de los documentos, puede ser utilizado en otros tipos de formatos, como por ejemplo disquetes, almacenamiento en teléfonos móviles, agendas electrónicas portátiles o similares, tarjetas Bluetooth, discos ópticos, CDs, etc.

La alternativa del teléfono móvil o de la agenda electrónica es especialmente interesante, ya que nada impide enviar el código de autenticidad del documento al teléfono móvil del comprador mediante, por ejemplo un SMS o tecnología WAP, y que a la hora de hacer valer dicho documento el comprador lo descargue en el lector/verificador/grabador a través de un enlace infrarrojo, radio (por ejemplo Bluetooth, SMS, etc.) o similar.

En este caso, como ya se ha indicado, la limitación la longitud del código de barras ya no es tal, por lo que podría utilizarse criptografía de clave pública sin problemas.

Se describe a continuación la manera de utilizar la criptografía pública para generar el código de autenticidad.

En primer lugar se selecciona la información

relevante, se codifica y se firma digitalmente con la clave secreta del operador de lector adecuado (el lector/verificador/grabador que se encargará de comprobar el documento tiene almacenada la correspondiente clave pública).

Después, el resultado anterior se cifra con la clave pública correspondiente al dispositivo verificador portátil asociado al documento (el dispositivo verificador portátil que se encargará de validar el documento tiene almacenada la correspondiente clave secreta).

Se expone a continuación el proceso de verificación.

Se realiza la lectura del código de autenticidad y se transmite al dispositivo verificador portátil, que lo descifra con su clave secreta y lo introduce en la lista de documentos validados (si ya estaba en la lista indicaría tal hecho al lector/verificador/grabador).

El citado lector/verificador/grabador recibe el descifrado anterior y comprueba la validez de la firma con la clave pública del operador de lector que generó el código de autenticidad. Si la firma es correcta, acepta el documento y en caso contrario lo rechaza.

Existen cuatro combinaciones posibles en el uso de la criptografía de clave pública para este fin que son el cifrado (firma) como se ha expuesto anteriormente, firma (firma), cifrado (cifrado) y firma (firma). Debe notarse que, aunque las cuatro son posibles, es preferible la primera, ya que minimiza los riesgos de ataque al sistema. En concreto, hace innecesaria la existencia de la clave secreta del operador de lector e impide la lectura del contenido del código de seguridad.

Otra de las ventajas del procedimiento de la invención es que permite generar documentos de un determinado tipo o servicio para dispositivos verificadores portátiles de distintos operadores. Esta funcionalidad posibilita que varios portales asociados a

distintos operadores de dispositivos verificadores portátiles puedan generar documentos para un mismo servicio.

Además, con la invención se asegura que los distintos servicios y operadores de dispositivos verificadores portátiles no puedan afectar al funcionamiento y a la seguridad de otros servicios y operadores para los que no estén autorizados. Además, permite el anonimato del usuario y puede ser utilizado por cualquier usuario que sea portador de una tarjeta inteligente convenientemente programada (dispositivo verificador portátil) pero no requiere de ninguna identificación personal del usuario (únicamente se precisa de una identificación de la tarjeta la cual podría ser impersonal y transferible).

Debe destacarse especialmente el hecho de que el procedimiento descrito es de fácil implantación con los sistemas actuales de expedición de tickets.

El procedimiento de expedición y validación de documentos de la presente invención puede utilizarse para muchos tipos de documentos en diversos servicios y aplicaciones. Ejemplos de tipos de documentos son tickets para cines, teatros, espectáculos, etc. en los cuales se puede contratar un servicio adicional (por ejemplo, de aparcamiento), tickets para trenes, autobuses, barcos y transportes en general en los que existe una fecha concreta de viaje y un revisor humano (no hay tarjeta de embarque), tickets de avión, en los cuales se ha de obtener una tarjeta de embarque, bonos de hotel, de festivales o similares en los que ni la fecha ni el destino están prefijados de antemano, tarjetas multiviaje de transporte metropolitano, tales como metro, autobús, ferrocarriles de cercanías en los que no hay ni fecha ni plaza previstas de antemano, cupones de promoción, cheques, boletos de lotería, etc.

A continuación se describe una realización preferida del procedimiento de la presente invención.

Se expone el caso particular en el que sólo existe un operador de tarjeta, que es el emisor de las mismas, y que, a su vez, hace las veces de operador de lector. Además, el sistema se utiliza para la venta de tickets por Internet para ser impresos en casa del cliente con una impresora estándar de 300 ppp.

Como dispositivos verificadores portátiles se emplean tarjetas MIFARE ProX personalizadas mediante una clave obtenida cifrando el número de serie de cada tarjeta mediante DES Triple con una clave maestra. De esta manera se evita tener que guardar en una base de datos la correspondencia entre el número de serie y la clave de tarjeta. Se programa en ellas todo el protocolo que debe mantener con el lector/verificador/grabador y se dota de una lista de tickets cancelados con el procedimiento de eliminación de la lista de los tickets caducados mediante la inserción en la tarjeta de un certificado de fechas. El coprocesador criptográfico de la tarjeta está especialmente indicado para esta tarea. Una vez las tarjetas se han personalizado, se proporcionan a los usuarios del sistema.

Cada portador de tarjeta puede entonces conectarse al portal de tickets que considere adecuado, seleccionando normalmente cuál es el de su interés, utilizando el medio de pago que permita el portal. Una vez el portal considere que la transacción es válida, envía los datos que deben incrustarse en el código de autenticidad del ticket (se supone que es un valor de 128 bits, más que suficiente para casi la totalidad de las aplicaciones) al operador de tarjetas y de lectores, que en este caso se supone que coinciden. También envía el identificador de la tarjeta del comprador y el identificador del grupo de lectores que son los encargados

de la verificación para que puedan seleccionarse las claves adecuadas. La transmisión se realiza por Internet mediante SSL para garantizar la integridad y la autenticidad de la misma.

El operador de tarjeta y lector realiza un primer cifrado DES Triple de los datos recibidos con la clave del grupo de lectores indicados. Puesto que el tamaño de bloque del algoritmo es de 64 bits, se realiza el cifrado encadenado en modo CBC de los dos bloques (128 bits). La clave del lector la obtiene cifrando (DES Triple) el identificador del lector con una clave maestra que sólo él conoce. Luego realiza un segundo cifrado DES Triple (también encadenado CBC) con la clave de la tarjeta inteligente del portador del ticket, que puede obtenerla, de manera análoga a la del lector, cifrando el identificador de tarjeta con una clave maestra. El resultado de estos dos cifrados es un bloque de 128 bits que constituye el código de autenticidad del ticket. Dicho código se devuelve al portal también vía SSL.

El portal de ticket genera una versión PDF del ticket que contiene, en dos códigos de barras de tipo code128, el código de autenticidad. El motivo por el que se usan dos códigos es que, para una resolución de impresión de 300 ppp, la longitud de un código de barras code128 es de unos 75 mm para una información aproximada de 64 bits, que se corresponde con la máxima anchura admitida por los lectores de códigos de barras económicos. Los códigos incluyen una información en claro de manera que hace irrelevante el orden de lectura de los mismos. El ticket también incluye una trascripción numérica de la información de los códigos, de manera que si éstos se deterioran, dicha información pueda ser introducida manualmente.

El ticket en formato PDF se envía al comprador del mismo, el cual puede imprimirlo en el acto en una

impresora estándar.

Una vez en la entrada del espectáculo, el portador del ticket lo entrega junto con su tarjeta al portero. El portero lee el código de barras y a continuación acerca la tarjeta inteligente al lector/grabador sin contactos. La información del código de barras se transfiere en ese momento a la tarjeta, que comprueba que no esté en su lista de tickets ya cancelados. Si lo estuviese, indicaría al lector tal hecho, para que el portero pueda actuar adecuadamente. Si el ticket no se encuentra en la lista de cancelados, lo añade a dicha lista, lo descifra con su clave y lo envía al lector. El lector lo descifra a su vez con su clave secreta y comprueba que los datos sean consistentes (fecha, sesión, asiento, etc.) Si así sucede, valida definitivamente la entrada al espectáculo. Antes de realizarse la transferencia de datos entre lector y tarjeta, se establece una identificación mutua fuerte basada en retos y se establece una clave de sesión que se utilizará para cifrar toda la comunicación.

Aunque es posible utilizar el sistema usando un único cifrado correspondiente a la tarjeta, no resulta recomendable dado que la respuesta de la tarjeta podría ser suplantada fácilmente, hecho que debilitaría considerablemente la seguridad del sistema.

Resulta evidente para el experto en la materia que este procedimiento es susceptible de numerosas variaciones y modificaciones, y que los detalles mencionados pueden ser sustituidos por otros técnicamente equivalentes, sin por ello apartarse del ámbito de protección definido por las reivindicaciones adjuntas.

REIVINDICACIONES:

1ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" mediante códigos de autenticidad y elementos verificadores portátiles con capacidad de procesado y almacenamiento de información y alta protección frente a lecturas o escrituras desautorizadas, caracterizado en que el código de autenticidad se genera específicamente para un verificador portátil concreto, indicado de forma directa o indirecta por el solicitante del documento, de manera que es innecesario cualquier registro de información en el elemento verificador portátil hasta el momento de la validación del documento e imprescindible la participación activa de dicho elemento de verificación portátil para dicha validación, almacenando el verificador portátil una lista de los documentos que ha validado, de manera que es posible saber, al menos, si se trata de la primera validación.

2ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la 1ª reivindicación caracterizado en que comprende las etapas de:

- individualización de los dispositivos verificadores portátiles por parte de sus emisores mediante una o varias claves de dispositivo verificador portátil;

- generación del documento desde un portal de documentos codificándose los datos que se consideren relevantes para realizar una primera operación criptográfica con la clave correspondiente de un grupo de lectores/verificadores/grabadores que participan en la validación del documento y, concatenada a la primera, una segunda operación criptográfica que involucra la clave correspondiente del dispositivo verificador portátil asociado al documento, constituyendo el resultado de dichas operaciones criptográficas un código de autenticidad del documento incorporado al mismo; y

- comprobación del documento que comprende la lectura del

código de autenticidad del mismo, realizándose unas terceras operaciones criptográficas adecuadas para la verificación de las utilizadas en la generación del documento, siendo imprescindible la participación activa del dispositivo verificador portátil asociado para la validación del documento y almacenando el verificador portátil una lista de los documentos que ha verificado de manera que es posible saber, al menos, si se trata de la primera validación.

3ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la 2ª reivindicación, caracterizado en que:

- la citada etapa de individualización de los dispositivos verificadores portátiles se realiza almacenando una o varias claves de dispositivo verificador portátil, siendo estas claves las de un algoritmo de cifrado simétrico o de clave secreta;
- dicha primera y segunda operación criptográfica comprenden dos cifrados mediante un algoritmo criptográfico simétrico con la clave del grupo de lectores/verificadores/grabadores que participan en la validación del documento y otro algoritmo criptográfico simétrico con la clave correspondiente del dispositivo verificador portátil asociado al documento; y en que
- dichas terceras operaciones criptográficas comprenden el descifrado, por parte del dispositivo verificador portátil con su clave correspondiente, del código de autenticidad del documento y el descifrado subsiguiente, por parte del citado lector/verificador/grabador con su clave correspondiente, realizándose ambos descifrados mediante algoritmos criptográficos simétricos.

4ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la 2ª reivindicación, caracterizado en que:

- la individualización de los dispositivos verificadores

portátiles se lleva a cabo almacenando una o varias claves de dispositivo verificador portátil, siendo estas claves las secretas de un algoritmo criptográfico asimétrico o de clave pública;

- la citada primera y segunda operación criptográfica se basa en criptografía de clave pública que comprende una firma digital con una clave secreta, de la cual los citados lectores/verificadores/grabadores que participan en la validación del documento conocen su correspondiente pública, y un cifrado con la clave pública correspondiente del dispositivo verificador portátil asociado al documento; y en que

- las citadas terceras operaciones criptográficas se basan en criptografía de clave pública que comprenden un descifrado con la clave secreta correspondiente del dispositivo verificador portátil asociado al documento y una comprobación de firma, con la clave pública correspondiente almacenada en los lectores/verificadores/grabadores.

5ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la 2ª reivindicación, caracterizado en que:

- la individualización de los dispositivos verificadores portátiles se lleva a cabo almacenando una o varias claves de dispositivo verificador portátil, siendo estas claves las secretas de un algoritmo criptográfico asimétrico o de clave pública;

- la citada primera y segunda operación criptográfica se basa en criptografía de clave pública que comprende un cifrado con la clave pública de los lectores/verificadores/grabadores que participan en la validación del documento y un cifrado con la clave pública correspondiente del dispositivo verificador portátil asociado al documento; y

-las citadas terceras operaciones criptográficas se basan

en criptografía de clave pública que comprenden un descifrado con la clave secreta correspondiente del dispositivo verificador portátil asociado al documento y una descifrado con la clave secreta de dichos lectores/verificadores/grabadores.

6ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la 2ª reivindicación, caracterizado en que:

- la individualización de los dispositivos verificadores portátiles se lleva a cabo almacenando una o varias claves de dispositivo verificador portátil, siendo estas claves las públicas de un algoritmo criptográfico asimétrico o de clave pública;

- dicha primera y segunda operación criptográfica se basan en criptografía de clave pública que comprende una firma digital con la clave secreta correspondiente a la clave pública almacenada en los citados lectores/verificadores/grabadores que participan en la validación del documento y otra firma digital con la clave secreta correspondiente a la clave de individualización adecuada almacenada en el dispositivo verificador portátil asociado al documento; y en que

- las citadas terceras operaciones criptográficas se basan en criptografía de clave pública que comprende la comprobación de firma por parte del dispositivo verificador portátil asociado al documento con su clave de individualización adecuada y otra comprobación de firma con la clave pública correspondiente de los lectores/verificadores/grabadores.

7ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la 2ª reivindicación, caracterizado en que:

- la individualización de los dispositivos verificadores portátiles se lleva a cabo almacenando una o varias claves de dispositivo verificador portátil, siendo estas claves

las públicas de un algoritmo criptográfico asimétrico o de clave pública;

- la citada primera y segunda operación criptográfica se basan en criptografía de clave pública que comprende un cifrado con la clave pública correspondiente a la clave secreta almacenada en dichos lectores/verificadores/grabadores que participan en la validación del documento y una firma digital con la clave secreta correspondiente a la clave de individualización adecuada almacenada en el dispositivo verificador portátil asociado al documento; y en que

- dichas terceras operaciones criptográficas se basan en criptografía de clave pública que comprende una comprobación de firma por parte del dispositivo verificador portátil asociado al documento con su clave de individualización adecuada y un descifrado con la clave secreta correspondiente de los citados lectores/verificadores/grabadores.

8ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según cualquiera de las reivindicaciones anteriores, caracterizado en que comprende la comprobación, antes de validar el documento, de que éste no se encuentra en la lista de documentos validados.

9ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la reivindicación 8ª, caracterizado en que comprende la indicación al lector/grabador/verificador de que el documento a validar se encuentra en la lista de documentos validados para que éste tome las medidas oportunas.

10ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la reivindicación 8ª, caracterizado en que comprende la inclusión del documento en la lista de documentos validados en el caso de que el documento a validar no se encuentre en la misma, realizándose la operación criptográfica correspondiente a invertir y/o

comprobar la operación criptográfica correspondiente al dispositivo verificador portátil, enviando el resultado al lector/grabador/verificador para que tome las medidas oportunas.

11ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la 2ª reivindicación, caracterizado en la autentificación criptográfica establecida entre el citado dispositivo verificador portátil y el lector/grabador/verificador es una autentificación criptográfica mutua fuerte.

12ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la reivindicación 11ª, caracterizado en que entre el dispositivo verificador portátil y el lector/grabador/verificador se establece una clave de sesión cooperativa y aleatoria utilizada para cifrar los mensajes pertinentes entre ambos.

13ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la reivindicación 2ª, caracterizado en que la etapa de individualización de los dispositivos verificadores portátiles por parte de sus emisores se realiza mediante una o varias claves que se obtienen a partir del cifrado del número de serie con una o varias claves maestras elegidas por los operadores de dispositivos verificadores portátiles, de manera que la clave maestra de cada operador y el dispositivo verificador portátil corresponde con su identificador, apareciendo dicho identificador de una manera legible para el usuario.

14ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la reivindicación 2ª, caracterizado en que el citado lector/verificador/grabador está adaptado para emitir una información admitiendo o rechazando el documento e informando de la causa.

15ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la reivindicación 2ª, caracterizado

en que las claves del lector/verificador/grabador son comunes a un conjunto de lectores.

16ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la 2ª reivindicación, caracterizado en que las claves almacenadas en los lectores/verificadorer/grabadores se obtienen cifrando sus identificadores o parte de ellos con unas claves maestras elegidas por sus operadores.

17ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la 1ª reivindicación, caracterizado en que en los documentos que presentan fecha de caducidad, ésta se incorpora en el código de autenticidad, de manera que pueden ser eliminados de la lista de documentos validados almacenada en dicho verificador portátil una vez que éstos han caducado.

18ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la reivindicación 17ª, caracterizado en que los citados dispositivos verificadores portátiles adquieren la fecha para borrar los documentos caducados de la lista de documentos validados por medio de un certificado digital emitido por una entidad competente.

19ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según cualquiera de las reivindicaciones anteriores, caracterizado en que la selección y obtención del documento y/o su código de autenticidad se realiza a través de Internet.

20ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según cualquiera de las reivindicaciones anteriores, caracterizado en que el código de autenticidad del documento se envía al teléfono móvil del usuario.

21ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según cualquiera de las reivindicaciones anteriores, caracterizado en que el código de autenticidad del documento se envía a una agenda electrónica o similar del usuario.

22ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según cualquiera de las reivindicaciones anteriores, caracterizado en que el código de autenticidad se imprime mediante un código de barras.

23ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según cualquiera de las reivindicaciones anteriores, caracterizado en que el código de autenticidad se imprime mediante varios código de barras.

24ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según cualquiera de las reivindicaciones anteriores, caracterizado en que el código de autenticidad se imprime mediante un código alfanumérico.

25ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según cualquiera de las reivindicaciones anteriores, caracterizado en que el código de autenticidad se imprime mediante un código de puntos.

26ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según cualesquiera de las reivindicaciones 22ª a 25ª, caracterizado en que el código de autenticidad se imprime también en modo alfanumérico para poder realizar una entrada manual del mismo en caso de deterioro del código de lectura automática.

27ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la reivindicación 23ª caracterizado en que en los códigos de barras incluyen el orden correcto de lectura.

(12) SOLICITUD INTERNACIONAL PUBLICADA EN VIRTUD DEL TRATADO DE COOPERACIÓN EN MATERIA DE PATENTES (PCT)

(19) Organización Mundial de la Propiedad Intelectual
Oficina internacional

(43) Fecha de publicación internacional
24 de Julio de 2003 (24.07.2003)

PCT

(10) Número de Publicación Internacional
WO 03/060782 A1

(51) Clasificación Internacional de Patentes[7]: G06F 17/60, H04L 9/00

(21) Número de la solicitud internacional: PCT/ES03/00008

(22) Fecha de presentación internacional:
10 de Enero de 2003 (10.01.2003)

(25) Idioma de presentación: español

(26) Idioma de publicación: español

(30) Datos relativos a la prioridad:
P200200070 15 de Enero de 2002 (15.01.2002) ES

(71) Solicitante *(para todos los Estados designados salvo US)*: **UNIVERSITAT POLITECNICA DE CATALUNYA** [ES/ES]; Jordi Girona Salgado, 31, Edificio C-H, E-08034 Barcelona (ES).

(72) Inventores; e

(75) Inventores/Solicitantes *(para US solamente)*: **RICO NOVELLA, Francisco, Jose** [ES/ES]; Jordi Girona-Salgado, 31, Edificio C-H, E-08034 Barcelona (ES). **FORGA ALBERICH, Jordi** [ES/ES]; Jordi Girona Salgado, 31, Edificio C-H, E-08034 Barcelona (ES). **SANICENTE GARGALLO, Emilio** [ES/ES]; Jordi Girona Salgado, 31, Edificio C-H, E-08034 Barcelona (ES). **MATA DIAZ, Jorge** [ES/ES]; Jordi Girona Salado, 31, Edificio C-H, E-08034 Barcelona (ES). **DE LA CRUZ LLOPIS, Luis, Javier** [ES/ES]; Jordi Girona Salagdo, 31, Edificio C-H, E-08034 Barcelona (ES). **ALINS DELGADO, Juan, Jose** [ES/ES]; Jordi Girona Salgado, 31, Edificio C-H, E-08034 Barcelona (ES).

(74) Mandatario: **MORGADES MANONELLES, Juan, Antonio**; Rector Ubach, 37-39 bajos 2ª, E-08021 Barcelona (ES).

(81) Estados designados *(nacional)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Estados designados *(regional)*: patente ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), patente euroasiática (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), patente europea (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), patente OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaraciónes según la Regla 4.17:

— *sobre la identidad del inventor (Regla 4.17(i)) para las siguientes designaciones AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW, patente ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), patente euroasiática (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), patente europea (AT, BE, BG, CH, CY, CZ,*

[Continúa en la página siguiente]

(54) Title: METHOD OF SENDING AND VALIDATING DOCUMENTS

(54) Título: PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS

(57) Abstract: The invention relates to a method of sending and validating documents using authentication codes and portable verifier elements which can process and store information and which offer a high level of protection against unauthorised readers and writers. The inventive method is characterised in that the aforementioned authentication code is generated specifically for a particular portable verifier and is indicated directly or indirectly by the person requesting the document. In this way, no data record of any type is required in the portable verifier element up to the point at which the document is validated. It is essential, however, that the portable verifier be actively involved in the validation, said portable verifier containing a stored list of validated documents such that it is possible to determine, at least, whether or not this is the first validation.

(57) Resumen: Se realiza mediante códigos de autenticidad y elementos verificadores portátiles con capacidad de procesado y almacenamiento de información y alta protección frente a lecturas o escrituras desautorizadas. Se caracteriza en que el código de autenticidad se genera específicamente para un verificador portátil concreto, indicado de forma directa o indirecta por el solicitante del documento, de manera que es innecesario cualquier registro de información en el elemento verificador portátil hasta el momento de la validación del documento e imprescindible la participación activa de dicho elemento de verificación portátil para dicha validación, almacenando el verificador portátil una lista de los documentos que ha validado, de manera que es posible saber, al menos, si se trata de la primera validación.

WO 03/060782 A1

DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), patente OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

— *sobre la identidad del inventor (Regla 4.17(i)) para las siguientes designaciones AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW, patente ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), patente euroasiática (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), patente europea (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), patente OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *sobre la identidad del inventor (Regla 4.17(i)) para las siguientes designaciones AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW, patente ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), patente euroasiática (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), patente europea (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), patente OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *sobre la identidad del inventor (Regla 4.17(i)) para las siguientes designaciones AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW, patente ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), patente euroasiática (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), patente europea (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), patente OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *sobre la identidad del inventor (Regla 4.17(i)) para las siguientes designaciones AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW, patente ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), patente euroasiática (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), patente europea (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), patente OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *sobre la identidad del inventor (Regla 4.17(i)) para las siguientes designaciones AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW, patente ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), patente euroasiática (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), patente europea (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), patente OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

Publicada:

— *con informe de búsqueda internacional*

Para códigos de dos letras y otras abreviaturas, véase la sección "Guidance Notes on Codes and Abbreviations" que aparece al principio de cada número regular de la Gaceta del PCT.

"PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS"

La presente invención hace referencia al procedimiento arriba indicado, con el cual resulta imposible la duplicación operativa de los mismos de manera fraudulenta. Tal como se detallará en lo sucesivo, el procedimiento que se describirá a continuación ofrece numerosas ventajas.

Aunque en la presente memoria se hace referencia esencialmente al caso en el que los documentos que se desean obtener son tickets, se entiende que el procedimiento objeto de la presente invención también es aplicable a otros tipos de documentos más generales, tal como se explicará más adelante.

Hoy en día es posible el encargo o la reserva de tickets tales como billetes de avión, billetes de tren, localidades de espectáculos y similares mediante sistemas de tele-venta. El procedimiento para el pago de los mismos es variado, pudiéndose realizar mediante el cargo a una tarjeta de crédito, a una cuenta a través de una entidad bancaria o similar.

Sin embargo, para recoger el ticket comprado de este modo era necesario que éste fuera enviado al destinatario por correo o mediante un servicio de mensajería, lo cual suponía un aumento en los costes de emisión y una incomodidad para el usuario si debía desplazarse para recoger los tickets.

Hasta ahora, la recogida del ticket se venía realizando de esta manera debido principalmente al hecho de que la autenticidad de este tipo de documento está basada en alguna característica del soporte (el papel) o del método de impresión para dificultar la falsificación del mismo. Esto impide que sea el propio usuario el que pueda obtener una copia impresa del documento.

Como alternativa a este procedimiento la técnica

anterior propone diversos sistemas de expedición de tickets de manera remota, los cuales se describen resumidamente a continuación.

Un primer sistema es el que se describe, en mayor o menor medida, en los documentos nº WO01/61577 A2, WO00/74300 A1, WO00/45348, WO200161577,WO2000744300, WO200045348, US5598477, el cual está basado esencialmente en la codificación de los datos que se consideran relevantes y su posterior cifrado, bien mediante técnicas de clave simétrica o asimétrica. El resultado de dicho cifrado se imprime en forma de código de barras o similar para poder realizar una comprobación automática cuando el ticket haya de ser validado. Este sistema imposibilita la generación de tickets por quien desconoce la clave de cifrado (si se usa criptografía de clave asimétrica, la clave secreta del algoritmo). Sin embargo, presenta el inconveniente de que es posible realizar copias de un ticket ya emitido y, por lo tanto, resulta necesario utilizar mecanismos adicionales de seguridad, tal como el control en línea de los tickets validados, la inclusión de información personal contrastable (DNI, pasaporte o similar) en el código cifrado (para aquellos tickets que presenten una fecha y un lugar fijos de utilización), etc. Este sistema es especialmente ineficaz en el caso de tickets que pueden ser utilizados en múltiples lugares y en un amplio abanico de fechas, como pueden ser bonos de noche en hoteles, bonos de transporte público, etc, así como en lugares de afluencia masiva, en los que el tiempo requerido para la comprobación de la identidad del portador resulta un serio inconveniente. Por todos estos motivos, este sistema no ha tenido demasiada implantación en la práctica.

Otro sistema es el que se describe, en mayor o menor medida, en los documentos nº EP0969426 A1, EP0829828 A, EP969426, JP11306397, EP309318 y otros, el cual está

basado en la grabación, en un dispositivo del tipo tarjeta inteligente, de la información del ticket. Debido a que el dispositivo de grabación (tarjeta) permite el uso de técnicas criptográficas para la identificación fuerte y presenta una gran robustez frente a la violación de la información que almacena, resulta prácticamente imposible duplicar el ticket, quedando la unicidad del mismo garantizada. Por lo tanto, resultan innecesarios tanto el control en línea de la validación del ticket como la identificación del portador cuando se consume. Sin embargo, este sistema presenta el inconveniente de que requiere que el usuario disponga de un periférico de grabación de tarjetas inteligentes en su casa, lo que encarece en gran medida el coste del sistema y hace que en la práctica no se utilice.

Una alternativa a los sistemas de expedición de tickets de manera remota es la que se propone con el nuevo procedimiento objeto de la presente invención, con el cual se consigue solventar los inconvenientes de los sistemas conocidos. La invención propone un nuevo procedimiento para la obtención de documentos (por ejemplo, tickets) típicamente en casa del usuario y su posterior validación automática. Con el procedimiento de la invención ya no es posible la duplicación operativa de los mismos (garantiza la unicidad) y hace innecesario que el usuario disponga de un lector/grabador de tarjetas inteligentes, lo que abarata y flexibiliza el sistema.

El procedimiento de la invención utiliza técnicas criptográficas robustas en conjunción con dispositivos verificadores portátiles, los cuales poseen capacidad de procesado y almacenamiento de información, presentan un alto grado de protección frente a lecturas y escrituras desautorizadas y dificultan en gran medida la duplicación fraudulenta.

Unos dispositivos verificadores portátiles que

resultan especialmente adecuados son las tarjetas inteligentes.

Aunque teóricamente resulta más adecuado el uso de criptografía de clave pública para la obtención de códigos de autenticidad (pues ello permite que en la fase de validación no se tengan que almacenar claves secretas), el tamaño de los códigos resultantes es sensiblemente superior al necesario si se emplea criptografía de clave secreta (simétrica). Si la forma final del documento no es impresa (soporte magnético, óptico, electrónico, etc.) este hecho no presenta mayor relevancia, pero si el documento ha de imprimirse, la lectura automática del código de autenticidad obligaría al uso de códigos de puntos, cuya lectura requiere aparatos más caros. Por este motivo, y para facilitar el soporte impreso, se prefiere el uso de criptografía de clave simétrica. Como contrapartida se tienen que utilizar dispositivos de almacenamiento seguro de claves en los verificadores, típicamente microprocesadores de seguridad.

La invención constituye un sistema seguro de expedición remota(típicamente por Internet desde un navegador) de documentos (típicamente tickets) y su validación mediante lectores automáticos (típicamente lectores de códigos de barras) capaces de leer/escribir en los dispositivos verificadores portátiles (típicamente tarjetas inteligentes). Por motivos de rapidez de lectura, robustez y versatilidad es recomendable que los dispositivos verificadores portátiles permitan la operación sin contactos.

Los elementos que intervienen en todo el procedimiento de la invención son los siguientes:

- emisor de dispositivos verificadores portátiles: es el encargado de proporcionar los dispositivos verificadores portátiles necesarios para la validación de los documentos.

- operador de dispositivos verificadores portátiles: realiza la parte del cifrado del documento que será descifrado por el dispositivo verificador portátil. Para poder realizar esta función las claves correspondientes deben de ser cargadas en el dispositivo verificador portátil. Un dispositivo verificador portátil puede soportar varios operadores de dispositivos verificadores portátiles. Un operador de dispositivo verificador portátil puede coincidir con un emisor.

- portal de documentos: es el encargado de proporcionar el interfaz necesario para la selección y, si procede, la compra del documento. Una vez seleccionado el documento el portal envía a un operador de lector la información adecuada para que sea cifrada con la clave del grupo de lectores/verificadores/grabadores que serán los encargados de validar el documento.

- operador de lector: es el encargado de realizar la parte del cifrado del documento que será descifrada por el citado grupo de lectores/verificadores/grabadores que serán los encargados de validar el documento. El operador de lector es el encargado de la gestión de las claves almacenadas en los lectores/verificadores/grabadores. Un operador de lector puede coincidir con un portal.

- lector/verificador/grabador: es el encargado de leer el código de autenticidad del documento, transmitirlo al dispositivo verificador portátil, recibir su respuesta, descifrarla con la clave correspondiente al operador de lector y validar o rechazar el documento.

- dispositivo verificador portátil: es el encargado de recibir el código de autenticidad del documento (transmitido por el lector/verificador/grabador), y si no ha sido previamente cancelado, descifrar con la clave correspondiente al operador de dispositivos verificadores portátiles,

incluirlo en su lista de cancelaciones y enviar al lector/verificador/grabador el resultado del descifrado.

El procedimiento de expedición y validación de documentos objeto de la presente invención se lleva a cabo mediante códigos de autenticidad y elementos verificadores portátiles con capacidad de procesado y almacenamiento de información y alta protección frente a lecturas o escrituras desautorizadas.

La particularidad de este procedimiento reside en el hecho de que el código de autenticidad se genera específicamente para un verificador portátil concreto, indicado de forma directa o indirecta por el solicitante del documento, de manera que es innecesario cualquier registro de información en el elemento verificador portátil hasta el momento de la validación del documento e imprescindible la participación activa de dicho elemento de verificación portátil para dicha validación, almacenando el verificador portátil una lista de los documentos que ha validado, de manera que es posible saber, al menos, si se trata de la primera validación.

El procedimiento de expedición y validación de documentos comprende las etapas de:

- generación del documento desde un portal de documentos codificándose los datos que se consideren relevantes para realizar una primera operación criptográfica con la clave correspondiente de un grupo de lectores/verificadores/grabadores que participan en la validación del documento y, concatenada a la primera, una segunda operación criptográfica que incluye la clave correspondiente del dispositivo verificador portátil asociado al documento, constituyendo el resultado de dichas operaciones criptográficas un código de autenticidad del documento incorporado al mismo; y

- comprobación del documento que comprende la lectura del código de autenticidad del mismo, realizándose

unas terceras operaciones criptográficas adecuadas para la verificación de las utilizadas en la generación del documento, siendo imprescindible la participación activa del dispositivo verificador portátil asociado para la validación del documento y almacenando el verificador portátil una lista de los documentos que ha verificado de manera que es posible saber, al menos, si se trata de la primera validación.

De acuerdo con una realización de la invención, la individualización de los dispositivos verificadores portátiles se realiza almacenando una o varias claves de dispositivo verificador portátil, siendo estas claves las de un algoritmo de cifrado simétrico o de clave secreta. Además, dicha primera y segunda operación criptográfica comprenden dos cifrados mediante un algoritmo criptográfico simétrico, uno con la clave del grupo de lectores/verificadores/grabadores que participan en la validación del documento y otro con la clave correspondiente del dispositivo verificador portátil asociado al documento; y las terceras operaciones criptográficas comprenden el descifrado, por parte del dispositivo verificador portátil con su clave correspondiente, del código de autenticidad del documento y el descifrado subsiguiente, por parte del citado lector/verificador/grabador con su clave correspondiente, realizándose ambos descifrados mediante algoritmos criptográficos simétricos.

Preferiblemente, la individualización de los dispositivos verificadores portátiles se lleva a cabo almacenando una o varias claves de dispositivo verificador portátil, siendo estas claves las secretas de un algoritmo criptográfico asimétrico o de clave pública. La citada primera y segunda operación criptográfica se basa en criptografía de clave pública que comprende una firma digital con una clave secreta, de la cual los citados

lectores/verificadores/grabadores que participan en la validación del documento conocen su correspondiente pública, y un cifrado con la clave pública correspondiente del dispositivo verificador portátil asociado al documento; y las terceras operaciones criptográficas se basan en criptografía de clave pública que comprenden un descifrado con la clave secreta correspondiente del dispositivo verificador portátil asociado al documento y una comprobación de firma, con la clave pública correspondiente almacenada en los lectores/verificadores/grabadores.

Alternativamente, la individualización de los dispositivos verificadores portátiles se lleva a cabo almacenando una o varias claves de dispositivo verificador portátil, siendo estas claves las secretas de un algoritmo criptográfico asimétrico o de clave pública. Dicha citada primera y segunda operación criptográfica se basa en criptografía de clave pública que comprende un cifrado con la clave pública de los lectores/verificadores/grabadores que participan en la validación del documento y un cifrado con la clave pública correspondiente del dispositivo verificador portátil asociado al documento. Las citadas terceras operaciones criptográficas se basan en criptografía de clave pública que comprenden un descifrado con la clave secreta correspondiente del dispositivo verificador portátil asociado al documento y una descifrado con la clave secreta de dichos lectores/verificadores/grabadores.

De acuerdo con otra característica alternativa de la presente invención, la individualización de los dispositivos verificadores portátiles se lleva a cabo almacenando una o varias claves de dispositivo verificador portátil, siendo estas claves las públicas de un algoritmo criptográfico asimétrico o de clave pública. La primera y segunda operación criptográfica se basan en criptografía

de clave pública que comprende una firma digital con la clave secreta correspondiente a la clave pública almacenada en los citados lectores/verificadores/grabadores que participan en la validación del documento y otra firma digital con la clave secreta correspondiente a la clave de individualización adecuada almacenada en el dispositivo verificador portátil asociado al documento, y las citadas terceras operaciones criptográficas se basan en criptografía de clave pública que comprende la comprobación de firma por parte del dispositivo verificador portátil asociado al documento con su clave de individualización adecuada y otra comprobación de firma con la clave pública correspondiente de los lectores/verificadores/grabadores.

Otra alternativa es que la individualización de los dispositivos verificadores portátiles se lleve a cabo almacenando una o varias claves de dispositivo verificador portátil, siendo estas claves las públicas de un algoritmo criptográfico asimétrico o de clave pública y que la primera y segunda operación criptográfica se basen en criptografía de clave pública que comprende un cifrado con la clave pública correspondiente a la clave secreta almacenada en dichos lectores/verificadores/grabadores que participan en la validación del documento y una firma digital con la clave secreta correspondiente a la clave de individualización adecuada almacenada en el dispositivo verificador portátil asociado al documento; y que dichas terceras operaciones criptográficas se basen en criptografía de clave pública que comprende una comprobación de firma por parte del dispositivo verificador portátil asociado al documento con su clave de individualización adecuada y un descifrado con la clave secreta correspondiente de los citados lectores/verificadores/grabadores.

Adicionalmente, el procedimiento de la invención

también comprende la comprobación, antes de validar el documento, de que éste no se encuentra en la lista de documentos validados.

También se realiza una indicación al lector/grabador/verificador de que el documento a validar se encuentra en la lista de documentos validados para que éste tome las medidas oportunas.

Se prevé asimismo la inclusión del documento en la lista de documentos validados en el caso de que el documento a validar no se encuentre en la misma, realizándose la operación criptográfica correspondiente a invertir y/o comprobar la operación criptográfica correspondiente al dispositivo verificador portátil, enviando el resultado al lector/grabador/verificador para que tome las medidas oportunas.

Ventajosamente, la autentificación criptográfica establecida entre el citado dispositivo verificador portátil y el lector/grabador/verificador es una autentificación criptográfica mutua fuerte.

Debe destacarse especialmente el hecho de que entre el dispositivo verificador portátil y el lector/grabador/verificador se establece una clave de sesión cooperativa y aleatoria utilizada para cifrar los mensajes pertinentes entre ambos.

Preferiblemente, la etapa de individualización de los dispositivos verificadores portátiles por parte de sus emisores se realiza mediante una o varias claves que se obtienen a partir del cifrado del número de serie con una o varias claves maestras elegidas por los operadores de dispositivos verificadores portátiles, de manera que la clave maestra de cada operador y el dispositivo verificador portátil corresponde con su identificador, apareciendo dicho identificador de una manera legible para el usuario.

De acuerdo con la invención, el citado

lector/verificador/grabador está adaptado para emitir una información admitiendo o rechazando el documento e informando de la causa.

Ventajosamente, las claves del lector/verificador/grabador son comunes a un conjunto de lectores.

Las claves almacenadas en los lectores/verificadores/grabadores se obtienen cifrando sus identificadores o parte de ellos con unas claves maestras elegidas por sus operadores.

Si los documentos presentan fecha de caducidad, ésta se incorpora en el código de autenticidad, de manera que pueden ser eliminados de la lista de documentos validados almacenada en dicho verificador portátil una vez que éstos han caducado.

Por otra parte, los citados dispositivos verificadores portátiles adquieren la fecha para borrar los documentos caducados de la lista de documentos validados por medio de un certificado digital emitido por una entidad competente.

La selección y obtención del documento y/o su código de autenticidad puede realizarse a través de Internet y el código de autenticidad del documento se puede enviar al teléfono móvil del usuario o una agenda electrónica o similar del usuario.

De acuerdo con otra característica de la invención, el código de autenticidad puede imprimirse mediante uno o varios códigos de barras. En el caso de varios códigos, éstos incluyen el orden correcto de lectura. Se prevé también que el código de autenticidad pueda imprimirse mediante un código alfanumérico o un código de puntos. El código de autenticidad puede imprimirse también en modo alfanumérico para poder realizar una entrada manual del mismo en caso de deterioro del código de lectura automática.

El procedimiento descrito garantiza la autenticidad y la unicidad de los documentos. Los cifrados del código de autenticidad se realizan utilizando un par de claves secretas. Esto asegura que no puedan generarse externamente documentos auténticos. La unicidad se consigue relacionando uno de los cifrados con el dispositivo verificador portátil. Si el documento se duplica por cualquier sistema, no se obtiene ningún resultado ya que el dispositivo verificador portátil, una vez que valida un documento, no vuelve a validarlo de nuevo. Por lo tanto, para sacar partido a la copia sería necesario duplicar el dispositivo verificador portátil y esto no es posible por sus características.

Por otra parte, es posible también la cancelación de documentos sin necesidad de transmisión de listas negras al lector/verificador/grabador. Para la cancelación, el titular del documento debe acudir a una oficina autorizada con el documento y el dispositivo verificador portátil. Para cancelar el documento, se cargará como anulado en el dispositivo verificador portátil de manera que, si el comprador ha guardado una copia del documento, no podrá usarlo puesto que ese dispositivo verificador portátil ya no lo validará.

La inclusión de listas de cancelación de documentos (si se desea que no se desborde la capacidad de almacenamiento del dispositivo verificador portátil) tiene varias implicaciones. Los documentos que caduquen deben incorporar la fecha de caducidad en el código de autenticidad, de manera que una vez hayan caducado puedan ser eliminados de la lista para liberar espacio. Los dispositivos verificadores portátiles deben incorporar un gestor de cancelaciones residuales, de manera que detecten los documentos caducados y realicen una limpieza a partir de la fecha obtenida de un certificado proporcionado por el lector/verificador/grabador. La fecha se obtiene de un

servidor central que certifica la misma mediante un sistema de clave pública. Dicho certificado, que puede ser emitido una única vez al día, se pasa al dispositivo verificador portátil que, después de comprobar su autenticidad, elimina de la lista los documentos cancelados que ya hayan caducado según la fecha certificada. Naturalmente un documento caducado no será nunca aceptado como válido.

Se trata de un sistema universal para múltiples servicios (espectáculos, transportes, abonos, cupones, cheques, boletos de lotería...), múltiples portales de Internet y múltiples operadores de dispositivos verificadores portátiles. Aunque el sistema es particularmente útil para el formato impreso de los documentos, puede ser utilizado en otros tipos de formatos, como por ejemplo disquetes, almacenamiento en teléfonos móviles, agendas electrónicas portátiles o similares, tarjetas Bluetooth, discos ópticos, CDs, etc.

La alternativa del teléfono móvil o de la agenda electrónica es especialmente interesante, ya que nada impide enviar el código de autenticidad del documento al teléfono móvil del comprador mediante, por ejemplo un SMS o tecnología WAP, y que a la hora de hacer valer dicho documento el comprador lo descargue en el lector/verificador/grabador a través de un enlace infrarrojo, radio (por ejemplo Bluetooth, SMS, etc.) o similar.

En este caso, como ya se ha indicado, la limitación la longitud del código de barras ya no es tal, por lo que podría utilizarse criptografía de clave pública sin problemas.

Se describe a continuación la manera de utilizar la criptografía pública para generar el código de autenticidad.

En primer lugar se selecciona la información

relevante, se codifica y se firma digitalmente con la clave secreta del operador de lector adecuado (el lector/verificador/grabador que se encargará de comprobar el documento tiene almacenada la correspondiente clave pública).

Después, el resultado anterior se cifra con la clave pública correspondiente al dispositivo verificador portátil asociado al documento (el dispositivo verificador portátil que se encargará de validar el documento tiene almacenada la correspondiente clave secreta).

Se expone a continuación el proceso de verificación.

Se realiza la lectura del código de autenticidad y se transmite al dispositivo verificador portátil, que lo descifra con su clave secreta y lo introduce en la lista de documentos validados (si ya estaba en la lista indicaría tal hecho al lector/verificador/grabador).

El citado lector/verificador/grabador recibe el descifrado anterior y comprueba la validez de la firma con la clave pública del operador de lector que generó el código de autenticidad. Si la firma es correcta, acepta el documento y en caso contrario lo rechaza.

Existen cuatro combinaciones posibles en el uso de la criptografía de clave pública para este fin que son el cifrado (firma) como se ha expuesto anteriormente, firma (firma), cifrado (cifrado) y firma (firma). Debe notarse que, aunque las cuatro son posibles, es preferible la primera, ya que minimiza los riesgos de ataque al sistema. En concreto, hace innecesaria la existencia de la clave secreta del operador de lector e impide la lectura del contenido del código de seguridad.

Otra de las ventajas del procedimiento de la invención es que permite generar documentos de un determinado tipo o servicio para dispositivos verificadores portátiles de distintos operadores. Esta funcionalidad posibilita que varios portales asociados a

distintos operadores de dispositivos verificadores portátiles puedan generar documentos para un mismo servicio.

Además, con la invención se asegura que los distintos servicios y operadores de dispositivos verificadores portátiles no puedan afectar al funcionamiento y a la seguridad de otros servicios y operadores para los que no estén autorizados. Además, permite el anonimato del usuario y puede ser utilizado por cualquier usuario que sea portador de una tarjeta inteligente convenientemente programada (dispositivo verificador portátil) pero no requiere de ninguna identificación personal del usuario (únicamente se precisa de una identificación de la tarjeta la cual podría ser impersonal y transferible).

Debe destacarse especialmente el hecho de que el procedimiento descrito es de fácil implantación con los sistemas actuales de expedición de tickets.

El procedimiento de expedición y validación de documentos de la presente invención puede utilizarse para muchos tipos de documentos en diversos servicios y aplicaciones. Ejemplos de tipos de documentos son tickets para cines, teatros, espectáculos, etc. en los cuales se puede contratar un servicio adicional (por ejemplo, de aparcamiento), tickets para trenes, autobuses, barcos y transportes en general en los que existe una fecha concreta de viaje y un revisor humano (no hay tarjeta de embarque), tickets de avión, en los cuales se ha de obtener una tarjeta de embarque, bonos de hotel, de festivales o similares en los que ni la fecha ni el destino están prefijados de antemano, tarjetas multiviaje de transporte metropolitano, tales como metro, autobús, ferrocarriles de cercanías en los que no hay ni fecha ni plaza previstas de antemano, cupones de promoción, cheques, boletos de lotería, etc.

A continuación se describe una realización preferida del procedimiento de la presente invención.

Se expone el caso particular en el que sólo existe un operador de tarjeta, que es el emisor de las mismas, y que, a su vez, hace las veces de operador de lector. Además, el sistema se utiliza para la venta de tickets por Internet para ser impresos en casa del cliente con una impresora estándar de 300 ppp.

Como dispositivos verificadores portátiles se emplean tarjetas MIFARE ProX personalizadas mediante una clave obtenida cifrando el número de serie de cada tarjeta mediante DES Triple con una clave maestra. De esta manera se evita tener que guardar en una base de datos la correspondencia entre el número de serie y la clave de tarjeta. Se programa en ellas todo el protocolo que debe mantener con el lector/verificador/grabador y se dota de una lista de tickets cancelados con el procedimiento de eliminación de la lista de los tickets caducados mediante la inserción en la tarjeta de un certificado de fechas. El coprocesador criptográfico de la tarjeta está especialmente indicado para esta tarea. Una vez las tarjetas se han personalizado, se proporcionan a los usuarios del sistema.

Cada portador de tarjeta puede entonces conectarse al portal de tickets que considere adecuado, seleccionando normalmente cuál es el de su interés, utilizando el medio de pago que permita el portal. Una vez el portal considere que la transacción es válida, envía los datos que deben incrustarse en el código de autenticidad del ticket (se supone que es un valor de 128 bits, más que suficiente para casi la totalidad de las aplicaciones) al operador de tarjetas y de lectores, que en este caso se supone que coinciden. También envía el identificador de la tarjeta del comprador y el identificador del grupo de lectores que son los encargados

de la verificación para que puedan seleccionarse las claves adecuadas. La transmisión se realiza por Internet mediante SSL para garantizar la integridad y la autenticidad de la misma.

El operador de tarjeta y lector realiza un primer cifrado DES Triple de los datos recibidos con la clave del grupo de lectores indicados. Puesto que el tamaño de bloque del algoritmo es de 64 bits, se realiza el cifrado encadenado en modo CBC de los dos bloques (128 bits). La clave del lector la obtiene cifrando (DES Triple) el identificador del lector con una clave maestra que sólo él conoce. Luego realiza un segundo cifrado DES Triple (también encadenado CBC) con la clave de la tarjeta inteligente del portador del ticket, que puede obtenerla, de manera análoga a la del lector, cifrando el identificador de tarjeta con una clave maestra. El resultado de estos dos cifrados es un bloque de 128 bits que constituye el código de autenticidad del ticket. Dicho código se devuelve al portal también vía SSL.

El portal de ticket genera una versión PDF del ticket que contiene, en dos códigos de barras de tipo code128, el código de autenticidad. El motivo por el que se usan dos códigos es que, para una resolución de impresión de 300 ppp, la longitud de un código de barras code128 es de unos 75 mm para una información aproximada de 64 bits, que se corresponde con la máxima anchura admitida por los lectores de códigos de barras económicos. Los códigos incluyen una información en claro de manera que hace irrelevante el orden de lectura de los mismos. El ticket también incluye una trascripción numérica de la información de los códigos, de manera que si éstos se deterioran, dicha información pueda ser introducida manualmente.

El ticket en formato PDF se envía al comprador del mismo, el cual puede imprimirlo en el acto en una

impresora estándar.

Una vez en la entrada del espectáculo, el portador del ticket lo entrega junto con su tarjeta al portero. El portero lee el código de barras y a continuación acerca la tarjeta inteligente al lector/grabador sin contactos. La información del código de barras se transfiere en ese momento a la tarjeta, que comprueba que no esté en su lista de tickets ya cancelados. Si lo estuviese, indicaría al lector tal hecho, para que el portero pueda actuar adecuadamente. Si el ticket no se encuentra en la lista de cancelados, lo añade a dicha lista, lo descifra con su clave y lo envía al lector. El lector lo descifra a su vez con su clave secreta y comprueba que los datos sean consistentes (fecha, sesión, asiento, etc.) Si así sucede, valida definitivamente la entrada al espectáculo. Antes de realizarse la transferencia de datos entre lector y tarjeta, se establece una identificación mutua fuerte basada en retos y se establece una clave de sesión que se utilizará para cifrar toda la comunicación.

Aunque es posible utilizar el sistema usando un único cifrado correspondiente a la tarjeta, no resulta recomendable dado que la respuesta de la tarjeta podría ser suplantada fácilmente, hecho que debilitaría considerablemente la seguridad del sistema.

Resulta evidente para el experto en la materia que este procedimiento es susceptible de numerosas variaciones y modificaciones, y que los detalles mencionados pueden ser sustituidos por otros técnicamente equivalentes, sin por ello apartarse del ámbito de protección definido por las reivindicaciones adjuntas.

REIVINDICACIONES:

1ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" mediante códigos de autenticidad y elementos verificadores portátiles con capacidad de procesado y almacenamiento de información y alta protección frente a lecturas o escrituras desautorizadas, caracterizado en que el código de autenticidad se genera específicamente para un verificador portátil concreto, indicado de forma directa o indirecta por el solicitante del documento, de manera que es innecesario cualquier registro de información en el elemento verificador portátil hasta el momento de la validación del documento e imprescindible la participación activa de dicho elemento de verificación portátil para dicha validación, almacenando el verificador portátil una lista de los documentos que ha validado, de manera que es posible saber, al menos, si se trata de la primera validación.

2ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la 1ª reivindicación caracterizado en que comprende las etapas de:

- individualización de los dispositivos verificadores portátiles por parte de sus emisores mediante una o varias claves de dispositivo verificador portátil;

- generación del documento desde un portal de documentos codificándose los datos que se consideren relevantes para realizar una primera operación criptográfica con la clave correspondiente de un grupo de lectores/verificadores/grabadores que participan en la validación del documento y, concatenada a la primera, una segunda operación criptográfica que involucra la clave correspondiente del dispositivo verificador portátil asociado al documento, constituyendo el resultado de dichas operaciones criptográficas un código de autenticidad del documento incorporado al mismo; y

- comprobación del documento que comprende la lectura del

código de autenticidad del mismo, realizándose unas terceras operaciones criptográficas adecuadas para la verificación de las utilizadas en la generación del documento, siendo imprescindible la participación activa del dispositivo verificador portátil asociado para la validación del documento y almacenando el verificador portátil una lista de los documentos que ha verificado de manera que es posible saber, al menos, si se trata de la primera validación.

3ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la 2ª reivindicación, caracterizado en que:

- la citada etapa de individualización de los dispositivos verificadores portátiles se realiza almacenando una o varias claves de dispositivo verificador portátil, siendo estas claves las de un algoritmo de cifrado simétrico o de clave secreta;
- dicha primera y segunda operación criptográfica comprenden dos cifrados mediante un algoritmo criptográfico simétrico con la clave del grupo de lectores/verificadores/grabadores que participan en la validación del documento y otro algoritmo criptográfico simétrico con la clave correspondiente del dispositivo verificador portátil asociado al documento; y en que
- dichas terceras operaciones criptográficas comprenden el descifrado, por parte del dispositivo verificador portátil con su clave correspondiente, del código de autenticidad del documento y el descifrado subsiguiente, por parte del citado lector/verificador/grabador con su clave correspondiente, realizándose ambos descifrados mediante algoritmos criptográficos simétricos.

4ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la 2ª reivindicación, caracterizado en que:

- la individualización de los dispositivos verificadores

portátiles se lleva a cabo almacenando una o varias claves de dispositivo verificador portátil, siendo estas claves las secretas de un algoritmo criptográfico asimétrico o de clave pública;

- la citada primera y segunda operación criptográfica se basa en criptografía de clave pública que comprende una firma digital con una clave secreta, de la cual los citados lectores/verificadores/grabadores que participan en la validación del documento conocen su correspondiente pública, y un cifrado con la clave pública correspondiente del dispositivo verificador portátil asociado al documento; y en que

- las citadas terceras operaciones criptográficas se basan en criptografía de clave pública que comprenden un descifrado con la clave secreta correspondiente del dispositivo verificador portátil asociado al documento y una comprobación de firma, con la clave pública correspondiente almacenada en los lectores/verificadores/grabadores.

5ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la 2ª reivindicación, caracterizado en que:

- la individualización de los dispositivos verificadores portátiles se lleva a cabo almacenando una o varias claves de dispositivo verificador portátil, siendo estas claves las secretas de un algoritmo criptográfico asimétrico o de clave pública;

- la citada primera y segunda operación criptográfica se basa en criptografía de clave pública que comprende un cifrado con la clave pública de los lectores/verificadores/grabadores que participan en la validación del documento y un cifrado con la clave pública correspondiente del dispositivo verificador portátil asociado al documento; y

-las citadas terceras operaciones criptográficas se basan

en criptografía de clave pública que comprenden un descifrado con la clave secreta correspondiente del dispositivo verificador portátil asociado al documento y una descifrado con la clave secreta de dichos lectores/verificadores/grabadores.

6ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la 2ª reivindicación, caracterizado en que:

- la individualización de los dispositivos verificadores portátiles se lleva a cabo almacenando una o varias claves de dispositivo verificador portátil, siendo estas claves las públicas de un algoritmo criptográfico asimétrico o de clave pública;

- dicha primera y segunda operación criptográfica se basan en criptografía de clave pública que comprende una firma digital con la clave secreta correspondiente a la clave pública almacenada en los citados lectores/verificadores/grabadores que participan en la validación del documento y otra firma digital con la clave secreta correspondiente a la clave de individualización adecuada almacenada en el dispositivo verificador portátil asociado al documento; y en que

- las citadas terceras operaciones criptográficas se basan en criptografía de clave pública que comprende la comprobación de firma por parte del dispositivo verificador portátil asociado al documento con su clave de individualización adecuada y otra comprobación de firma con la clave pública correspondiente de los lectores/verificadores/grabadores.

7ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la 2ª reivindicación, caracterizado en que:

- la individualización de los dispositivos verificadores portátiles se lleva a cabo almacenando una o varias claves de dispositivo verificador portátil, siendo estas claves

las públicas de un algoritmo criptográfico asimétrico o de clave pública;

- la citada primera y segunda operación criptográfica se basan en criptografía de clave pública que comprende un cifrado con la clave pública correspondiente a la clave secreta almacenada en dichos lectores/verificadores/grabadores que participan en la validación del documento y una firma digital con la clave secreta correspondiente a la clave de individualización adecuada almacenada en el dispositivo verificador portátil asociado al documento; y en que

- dichas terceras operaciones criptográficas se basan en criptografía de clave pública que comprende una comprobación de firma por parte del dispositivo verificador portátil asociado al documento con su clave de individualización adecuada y un descifrado con la clave secreta correspondiente de los citados lectores/verificadores/grabadores.

8ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según cualquiera de las reivindicaciones anteriores, caracterizado en que comprende la comprobación, antes de validar el documento, de que éste no se encuentra en la lista de documentos validados.

9ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la reivindicación 8ª, caracterizado en que comprende la indicación al lector/grabador/verificador de que el documento a validar se encuentra en la lista de documentos validados para que éste tome las medidas oportunas.

10ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la reivindicación 8ª, caracterizado en que comprende la inclusión del documento en la lista de documentos validados en el caso de que el documento a validar no se encuentre en la misma, realizándose la operación criptográfica correspondiente a invertir y/o

comprobar la operación criptográfica correspondiente al dispositivo verificador portátil, enviando el resultado al lector/grabador/verificador para que tome las medidas oportunas.

11ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la 2ª reivindicación, caracterizado en la autentificación criptográfica establecida entre el citado dispositivo verificador portátil y el lector/grabador/verificador es una autentificación criptográfica mutua fuerte.

12ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la reivindicación 11ª, caracterizado en que entre el dispositivo verificador portátil y el lector/grabador/verificador se establece una clave de sesión cooperativa y aleatoria utilizada para cifrar los mensajes pertinentes entre ambos.

13ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la reivindicación 2ª, caracterizado en que la etapa de individualización de los dispositivos verificadores portátiles por parte de sus emisores se realiza mediante una o varias claves que se obtienen a partir del cifrado del número de serie con una o varias claves maestras elegidas por los operadores de dispositivos verificadores portátiles, de manera que la clave maestra de cada operador y el dispositivo verificador portátil corresponde con su identificador, apareciendo dicho identificador de una manera legible para el usuario.

14ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la reivindicación 2ª, caracterizado en que el citado lector/verificador/grabador está adaptado para emitir una información admitiendo o rechazando el documento e informando de la causa.

15ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la reivindicación 2ª, caracterizado

en que las claves del lector/verificador/grabador son comunes a un conjunto de lectores.

16ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la 2ª reivindicación, caracterizado en que las claves almacenadas en los lectores/verificadorer/grabadores se obtienen cifrando sus identificadores o parte de ellos con unas claves maestras elegidas por sus operadores.

17ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la 1ª reivindicación, caracterizado en que en los documentos que presentan fecha de caducidad, ésta se incorpora en el código de autenticidad, de manera que pueden ser eliminados de la lista de documentos validados almacenada en dicho verificador portátil una vez que éstos han caducado.

18ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la reivindicación 17ª, caracterizado en que los citados dispositivos verificadores portátiles adquieren la fecha para borrar los documentos caducados de la lista de documentos validados por medio de un certificado digital emitido por una entidad competente.

19ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según cualquiera de las reivindicaciones anteriores, caracterizado en que la selección y obtención del documento y/o su código de autenticidad se realiza a través de Internet.

20ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según cualquiera de las reivindicaciones anteriores, caracterizado en que el código de autenticidad del documento se envía al teléfono móvil del usuario.

21ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según cualquiera de las reivindicaciones anteriores, caracterizado en que el código de autenticidad del documento se envía a una agenda electrónica o similar del usuario.

22ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según cualquiera de las reivindicaciones anteriores, caracterizado en que el código de autenticidad se imprime mediante un código de barras.

23ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según cualquiera de las reivindicaciones anteriores, caracterizado en que el código de autenticidad se imprime mediante varios código de barras.

24ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según cualquiera de las reivindicaciones anteriores, caracterizado en que el código de autenticidad se imprime mediante un código alfanumérico.

25ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según cualquiera de las reivindicaciones anteriores, caracterizado en que el código de autenticidad se imprime mediante un código de puntos.

26ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según cualesquiera de las reivindicaciones 22ª a 25ª, caracterizado en que el código de autenticidad se imprime también en modo alfanumérico para poder realizar una entrada manual del mismo en caso de deterioro del código de lectura automática.

27ª- "PROCEDIMIENTO DE EXPEDICIÓN Y VALIDACIÓN DE DOCUMENTOS" según la reivindicación 23ª caracterizado en que en los códigos de barras incluyen el orden correcto de lectura.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/ ES03/00008

A. CLASSIFICATION OF SUBJECT MATTER

IPC[7] G06F 17/60, H04L 9/00
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC[7] G06F +, H04L +

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CIBEPAT, EPODOC, WPI, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5341428 (Vernon L. Schatz et al.), 23.08.1994, * Column 3, line 30-column 6, line 3; column 7, line 54-column 8, line 56; figures*	1-7,13,14, 17,22-26
A	WO 0161577 A (MINDS), 23.08.2001, * **The whole document** *	1-10,14, 15,19-27
A	WO 0045348 A (JANG), 03.08.2000, * Page 3, line 18-page 5, line 30; page 6, line 14-32; figure*	1-10,14, 19,22,23
A	EP 0969426 A (SUN MICROSYSTEMS INC.), 05.01.2000, *Column 3, line 19-column 11, line 12; figures*	1-7,11, 13,19

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
05 March 2003 (05.03.03)	**07 April 2003 (07.04.03)**
Name and mailing address of the ISA/ **SPTO** Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/ ES03/00008

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	GB 2360384 A (NCR International, Inc.), 19.09.2001, *Page 10, line 24- page 20, line 22; figures*	1-9,19,22,23,26

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/ ES03/00008

Patent document cited in search report	Publication date	Patent familiy member(s)	Publication date
US 5341428	23.08.1994	CA 2088321 A	31.07.1993
WO 0161577 A	23.08.2001	AU 3715101 A BE 1013114 A	27.08.2001 04.09.2001
WO 0045348 A	03.08.2000	KR 2000023866A AU 1585400 A	06.05.2000 18.08.2000
EP 0969426 A	05.01.2000	JP 2000057210 A US 6216227 B DE 69901585 D DE 69901585 T	25.02.2000 10.04.2001 04.07.2002 07.11.2002
GB 2360384 A	19.09.2001	US 2001023893A	27.09.2001

INFORME DE BÚSQUEDA INTERNACIONAL

Solicitud internacional nº
PCT/ ES03/00008

A. CLASIFICACIÓN DEL OBJETO DE LA SOLICITUD

CIP[7] G06F 17/60, H04L 9/00
De acuerdo con la Clasificación Internacional de Patentes (CIP) o según la clasificación nacional y la CIP.

B. SECTORES COMPRENDIDOS POR LA BÚSQUEDA

Documentación mínima consultada (sistema de clasificación, seguido de los símbolos de clasificación)

CIP[7] G06F +, H04L +

Otra documentación consultada, además de la documentación mínima, en la medida en que tales documentos formen parte de los sectores comprendidos por la búsqueda

Bases de datos electrónicas consultadas durante la búsqueda internacional (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)
CIBEPAT, EPODOC, WPI, PAJ

C. DOCUMENTOS CONSIDERADOS RELEVANTES

Categoría*	Documentos citados, con indicación, si procede, de las partes relevantes	Relevante para las reivindicaciones nº
A	US 5341428 (Vernon L. Schatz et al.), 23.08.1994, * Columna 3, línea 30-columna 6, línea 3; columna 7, línea 54-columna 8, línea 56; figuras*	1-7,13,14,17,22-26
A	WO 0161577 A (MINDS), 23.08.2001, * Todo el documento*	1-10,14,15,19-27
A	WO 0045348 A (JANG), 03.08.2000, * Página 3, línea 18-página 5, línea 30; página 6, línea 14-32; figura*	1-10,14,19,22,23
A	EP 0969426 A (SUN MICROSYSTEMS INC.), 05.01.2000, *Columna 3, línea 19-columna 11, línea 12; figuras*	1-7,11,13,19

☒ En la continuación del recuadro C se relacionan otros documentos ☒ Los documentos de familia de patentes se indican en el anexo

* Categorías especiales de documentos citados:

"A" documento que define el estado general de la técnica no considerado como particularmente relevante.

"E" solicitud de patente o patente anterior pero publicada en la fecha de presentación internacional o en fecha posterior.

"L" documento que puede plantear dudas sobre una reivindicación de prioridad o que se cita para determinar la fecha de publicación de otra cita o por una razón especial (como la indicada).

"O" documento que se refiere a una divulgación oral, a una utilización, a una exposición o a cualquier otro medio.

"P" documento publicado antes de la fecha de presentación internacional pero con posterioridad a la fecha de prioridad reivindicada.

"T" documento ulterior publicado con posterioridad a la fecha de presentación internacional o de prioridad que no pertenece al estado de la técnica pertinente pero que se cita por permitir la comprensión del principio o teoría que constituye la base de la invención.

"X" documento particularmente relevante; la invención reivindicada no puede considerarse nueva o que implique una actividad inventiva por referencia al documento aisladamente considerado.

"Y" documento particularmente relevante; la invención reivindicada no puede considerarse que implique una actividad inventiva cuando el documento se asocia a otro u otros documentos de la misma naturaleza, cuya combinación resulta evidente para un experto en la materia.

"&" documento que forma parte de la misma familia de patentes.

Fecha en que se ha concluido efectivamente la búsqueda internacional. 05.marzo.2003 (05.03.2003)	Fecha de expedición del informe de búsqueda internacional 07 ABR 2003 07.04.03
Nombre y dirección postal de la Administración encargada de la búsqueda internacional O.E.P.M. C/Panamá 1, 28071 Madrid, España. nº de fax +34 91 3495304	Funcionario autorizado María José Lloris Meseguer nº de teléfono + 34 91 3495494

INFORME DE BUSQUEDA INTERNACIONAL

Solicitud internacional nº

PCT/ ES03/00008

C (Continuación). DOCUMENTOS CONSIDERADOS RELEVANTES

Categoría *	Documentos citados, con indicación, si procede, de las partes relevantes	Relevante para las reivindicaciones nº
A	GB 2360384 A (NCR International, Inc.), 19.09.2001, *Página 10, línea 24-página 20, línea 22; figuras*	1-9,19,22,23,26

INFORME DE BUSQUEDA [redacted] ERNACIONAL

Información relativa a miembros de familias de patentes

Solicitud [redacted] nacional nº PCT/ES03/00008

Documento de patente citado en el informe de búsqueda	Fecha de publicación	Miembro(s) de la familia de patentes	Fecha de publicación
US 5341428	23.08.1994	CA 2088321 A	31.07.1993
WO 0161577 A	23.08.2001	AU 3715101 A BE 1013114 A	27.08.2001 04.09.2001
WO 0045348 A	03.08.2000	KR 2000023866A AU 1585400 A	06.05.2000 18.08.2000
EP 0969426 A	05.01.2000	JP 2000057210 A US 6216227 B DE 69901585 D DE 69901585 T	25.02.2000 10.04.2001 04.07.2002 07.11.2002
GB 2360384 A	19.09.2001	US 2001023893A	27.09.2001